State of California

INSTRUCTIONS

**Plan Inventory for Existing
Continuity/Contingency Efforts**

v. 1.0

June 1, 1999

Plan Inventory for Existing Continuity/Contingency Efforts

DOIT recognizes that many State entities have already developed plans for potential disruptions to business operations. DOIT encourages use of these plans to the extent they address continuation of critical business processes. Making a *Plan Inventory* will assist in identifying which existing business continuity, contingency, resumption, disaster recovery plans, etc. can contribute to the completion of the CPB effort. The inventory should focus on the validity, relevance and overall applicability of the existing plans to meeting the process-oriented objectives of CPB. After completing section *3.0 Processes*, refer to the *Existing Plan Assessment Guide* to help assess the extent to which the existing plan(s) might contribute to the CPB effort.

The Plan Inventory document (MS Excel spreadsheet) is available in electronic form on the DOIT Year 2000 web page: http://www.year2000.ca.gov/. Please complete the electronic form and return it to the Y2K PMO at project.office@emc.ca.gov, including "Plan Inventory" in the subject line. **The completed Plan Inventory must be submitted to the Y2K PMO by June 21.**

Existing Continuity / Contingency Plans Inventory

		2.0 Plan Details			3.0 Processes				4.0 Systems		
		2.1 Type of Plan	2.2 Date Developed	2.3 Date Last Updated / Validated	3.1 Core Business Processes Mapped	3.2 Interim Processing Addressed	3.3 Business Process Resumption Addressed	3.4 Risk Reduction Addressed	4.1 Mission Critical Systems Addressed	4.2 System Processing Recovery Addressed	4.3 Data Recovery Addressed
1.0 Document Name											
[plan name]	Example	Disaster Recover	05/15/99	05/30/99	No	No	No	Yes	Yes	Yes	Yes
[plan name]											
[plan name]											
[plan name]											
[plan name]											
[plan name]											

5.0-Comments
[insert comments here]

This inventory schedule collects basic, high level information on any continuity/contingency plans that the entity has already developed. This information is useful to discern which plans provide continuity of services and processes, versus those that only provide for the recovery of information systems and data.

Any questions about the CPB Plan Inventory should be directed to the PMO at (916) 464-3688 or through e-mail at project.office@emc.ca.gov.

1.0 Document Name - List all related plans the entity has documented. Include any continuity, contingency, disaster recovery, operational recovery or similar plans that support the continuation of the entity's mission-critical or department-critical services. The definition of mission-critical and department-critical is available on the Y2K homepage at http://www.year2000.ca.gov/.

2.0 Plan Details - For each plan, provide information on the following:

2.1 Type of Plan - Identify the type of plan, such as contingency, continuity, disaster recovery, operational recovery plan, business resumption, etc.

2.2 Date Developed - Enter the date the plan was originally developed.

2.3 Date Last Updated/Validated - Enter the date the plan was last validated or updated.

3.0 Processes - This area documents whether existing plans address continuity of core business processes. An entity's plan(s) must address the continued delivery of its services. For each plan, answer the following questions:

3.1 Map Core Business Processes – Does the plan document what the core business processes are and how they work? This can include narratives or flow charts of the core business functions for each entity or department. *For additional information about mapping core business processes, please refer to the DOIT CPB Reference Guide - Section 2.1*

3.2 Interim Processing – Interim processing refers to those steps put in place to make sure service is delivered at least at an acceptable level while ability to resume normal processing is being established. Does the plan address interim processing requirements for core business processes? Contingency planning involves identifying alternate ways of operating the business process assuming the loss of specific assets and resources normally available to the business operation. Contingency planning includes the activities and resources required to bring operations back up to at least the

lowest acceptable level of service delivery, making sure essential services are delivered until normal operations are resumed. This planning is undertaken in response to a risk that cannot be easily reduced.

3.3 **Business Process Resumption Planning** – Does the plan address resuming core business operations back to the normal levels? Resumption Planning involves identifying the manner in which normal operations are restored. It focuses on the additional efforts that will bring the entity back to normal operating levels, assuming processes have been operating under contingency procedures for some time.

3.4 **Risk Reduction -** Does the plan have risk reduction components? Risk Reduction involves targeting certain critical, high-impact risks and designing action steps to reduce or eliminate the risk. The goal is to change the nature of the risk so that it no longer represents a serious threat to business operations.

4.0 **Systems** - This section assesses the information systems and data recovery components of the plans. For each documented plan, record the following information:

4.1 **Mission Critical Systems** - Does the plan address *mission critical* systems, as defined by DOIT?

4.2 **System Processing Recovery** - Does the plan address how the system(s) will resume processing (e.g. hot-sites, shared data centers) and be available for end users?

4.3 **Data Recovery** - Does the plan address how data will be recovered or restored?

5.0 **Comments** - Use this section to provide any additional information about existing plans.